EXHIBIT 115

Automotive News

TO SERVE AND PROTECT

Dealerships work to safeguard data as security breaches loom

David Barkholz

Automotive News | March 9, 2015 12:01 am EST

Today, practices designed to protect customer data are becoming commonplace as regulators increasingly view auto dealerships as financial institutions in terms of the magnitude of personal consumer information collected in the F&I department.

Eight years ago, Uftring Auto Group controller Patrick McKinley decided it was a bad idea from a data security standpoint to allow software vendors and companies that extract data for automakers direct access to the group's computers each night.

So he revamped his data sharing process, creating a scheme in which data from the group's main computer system are pushed to a lone, unconnected PC for harvesting by the companies that need it. Only the data fields that a specific vendor needs for a specific purpose are pushed out each day to the isolated PC.

At the time, McKinley stood apart.


McKinley: Early adopter

All dealerships need to share data automakers regularly require parts, inventory and certain transactional data, and third party vendors from direct mail marketers to inventory management companies need customer data to do their jobs. But for a store go to such lengths to protect consumer financial data against the slight risk they might leak to unauthorized people or otherwise get misused was unusual, and probably would have been seen as excessive.

Today, though, practices such as McKinley's are becoming commonplace as regulators increasingly view auto dealerships as financial institutions in terms of the magnitude of personal consumer information collected in the F&I department.

"We don't let anybody into our system because once the information gets out, you really don't know where it's going," McKinley said. Uftring sells 11 brands via six stores near Peoria, Ill.

Good stewardship

Even before the retail world was rocked by high profile personal data thefts from The Home Depot last year and Target in 2013, car dealers, their associations, vendors and automakers have been on a campaign to educate participants on good data stewardship.

With good reason, said Brad Miller, director of legal and regulatory affairs for the National Automobile Dealers Association.

Dealerships gather lots of nonpublic personal information from customers, especially in the F&I office, Miller said. That information includes credit applications, Social Security numbers, financing terms and other data that consumers expect won't be shared with, or fall into the hands of, anyone except the persons involved in their vehicle purchase.

Data breaches or even failure to have proper data handling processes could leave stores open to regulatory fines or worse, he said.

To date, the industry has avoided high visibility problems. But a data breach at a dealership would reflect badly on a store and, by extension, on the brand whose products are sold there, he said.

"Dealers have been relatively lucky," he said.

Vendors of dealer management systems and other software firms have been on the front lines of the industry fight to ensure that car companies and service providers get sufficient information to serve customers while safeguarding their personal information.

A dealer management system, or DMS, is the main operating software of a dealership. It houses payroll, accounting, inventory management, parts, service and often customer relationship management tools. It also typically stores all customer information.

The industry's dominant dealer management system vendors are CDK Global and Reynolds and Reynolds, which together provide DMS systems to about 80 percent of franchised stores. Both companies require their dealership clients' software and service providers to undergo aggressive certification programs.

A major cog of certification is a vendor's ability to safeguard dealership data, said Bob Schaefer, vice president of data services and OEM sales at Reynolds and Reynolds.

To obtain certification, any vendor interacting with a dealer management system provided by Reynolds must demonstrate its protocols for handling data.

That includes buttoned down contracts detailing how data will be used, whether they will be shared and the understanding that the data flow is subject to audit by Reynolds, Schaefer said.

The last item is critical because a dealership and its DMS vendor could be held responsible should customer data fall into unauthorized hands, he said. Periodic audits to test whether processes and employee training are being adhered to can prevent problems.

Schaefer said he has seen a discernible trend of dealerships that have moved, like McKinley, to pushing data out from their systems for harnessing rather than allowing vendors into their systems via pass codes.

Push it

He said that today, almost half of dealerships with a Reynolds DMS push out their data vs. only a handful of big customers a few years ago. He added that dealers and Reynolds don't want third parties "to rummage around" in the DMS.

It takes work for dealers to set up the push process and then load the necessary reports and data fields into the system each day, Schaefer said. But McKinley said it is worth the effort for Uftring to know exactly what data are going out of the system and to whom.

The other way vendors and automakers get data from dealers is to pull them, either by gaining direct access to the data via secure links and pass codes or by having third party vendors extract them on a regular basis.

CDK Global owns two of the largest data extraction contractors in the industry, Digital Motorworks Inc. and IntegraLink. The two contract with automakers and service vendors to pull data from dealerships with the permission of the dealers. Digital Motorworks and IntegraLink have made data security a top priority, building it into every aspect of how they extract, collate and distribute the data, according to Malcolm Thorne, CDK Global's chief strategy officer. The pull process of extracting data is as safe as pushing out, he said.

CDK Global has certified 120 vendors though its dealership data safeguarding program, Thorne said. Moreover, CDK Global launched a product, Dealer Data Exchange, at the NADA convention in January that gives a dealership the ability to see all data that leave the store, whether pushed out or extracted, he said.

Increasingly, dealerships are looking to provide shoppers with the convenience of doing more F&I functions online, including filling out credit applications, getting specific loan quotes and signing electronic contracts.

That's creating special challenges for companies such as Dealertrack Technologies, which is a leader in online retail software as well as in helping dealers match car buyers with banks.

With the encryption capabilities that Dealertrack uses and the electronic firewalls it builds around stores, the online environment is more secure for transferring data than are paper documents, faxes and overnight shipments, said Michael Collins, senior vice president of F&I solutions at Dealertrack.

Uftring's McKinley said he trusts pushing his data to vendors and is comfortable that they're only being used for authorized purposes. For example, he pushes data to vendors that identify service customers with equity in their vehicles (making them good new car candidates) and to automaker marketing vendors that send mailers on vehicle specials. Even so, he "salts" the data pushed out with his vacation address, personal email and his dog's name. Should he get a card or email addressed to "Barney McKinley" from a vendor he didn't authorize to use store data, he'll know they were shared by or taken from the vendor required to safeguard the information. "If something shows up," he said, "I'll be able to see where it came from."